

Audit

Report



COMPUTER SECURITY FOR THE
DEFENSE CIVILIAN PAY SYSTEM.

Report Number 99-128

April 8, 1999

Office of the Inspector General
Department of Defense

AQI 99-11-2136

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: **Computer Security for the Defense Civilian Pay System**

B. DATE Report Downloaded From the Internet: **08/23/99**

**C. Report's Point of Contact: (Name, Organization, Address, Office
Symbol, & Ph #):** **OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884**

D. Currently Applicable Classification Level: **Unclassified**

E. Distribution Statement A: **Approved for Public Release**

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ Preparation Date 08/23/99

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

19990824 134

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932 or visit the Inspector General, DoD, Home Page at: www.dodig.osd.mil.

Suggestions for Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ADPSSO	Automated Data Processing Special Security Officer
AIS	Automated Information System
CA-ACF2	Computer Associates International, Inc., Access Control Facility 2
DAC	Defense Information Systems Agency Area Command
DCPS	Defense Civilian Pay System
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DMC	Defense Megacenter
SEO	Systems Engineering Organization
GSO	Global System Option
ID	Identification
ISSO	Information System Security Officer
MVS	Multiple Virtual Storage
SSO	System Support Office
TIG	Technical Implementation Guide



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

April 8, 1999

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY

SUBJECT: Audit Report on Computer Security for the Defense Civilian Pay System
(Report No. 99-128)

We are providing this final report for review and comments. We considered management comments on a draft of this report when preparing the final report. This is our second audit report on security software and application controls over the Defense Civilian Pay System.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Defense Finance and Accounting Service comments conformed to the requirements of DoD Directive 7650.3; therefore, additional comments are not required from that organization. The Defense Information Systems Agency comments were partially responsive. We request that the Defense Information Systems Agency provide additional comments on Recommendations C.2.a. and C.2.b. by June 7, 1999.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Mr. Brian M. Flynn at (703) 604-9145 (DSN 664-9145) (BFlynn@dodig.osd.mil) or Mr. W. Andy Cooley at (303) 676-7393 (DSN 926-7393) (WCooley@dodig.osd.mil). See Appendix C for the report distribution. The audit team members are listed inside the back cover.

A handwritten signature in black ink, reading "Robert J. Lieberman", is positioned above the typed name.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-128
(Project No. 7FD-2023.01)

April 8, 1999

Computer Security for the Defense Civilian Pay System

Executive Summary

Introduction. This is the second audit of security software controls for the Defense Civilian Pay System, a civilian pay application. In FY 1991, the Defense Civilian Pay System was approved as the migratory civilian pay system for DoD. The application serves 733,000 employees and processes more than \$38 billion in payroll transactions annually. Employee pay records and account data are maintained by the Defense Finance and Accounting Service (DFAS) Denver Center, Denver, Colorado, and DFAS Operating Locations in Charleston, South Carolina, and Pensacola, Florida. Computer programming support is provided by the DFAS Systems Engineering Organization, Pensacola. The Defense Information Systems Agency Area Command, Mechanicsburg, Pennsylvania, and Systems Support Office, Dayton, Ohio, provide computer support for the pay data maintained by DFAS.

Objectives. The primary audit objective was to determine whether security software controls over the Defense Civilian Pay System adequately safeguarded the data integrity of employee payroll records. The audit also evaluated the management control program of DFAS and the Defense Information Systems Agency related to the other audit objectives.

Results. DFAS and the Defense Information Systems Agency needed to improve computer security over the Defense Civilian Pay System and its mainframe computers.

- Global System Option settings, which contain the standard system-wide security control options, were not established on the mainframe computers used for civilian pay processing in accordance with standard guidance. In addition, user access to sensitive privileges and mandatory password requirements was not adequately controlled. As a result, the Defense Information Systems Agency could not ensure the integrity of the mainframe computers that support the civilian pay application (Finding A).
- Inactive user identifications were not deleted from the production processing platforms for civilian pay when user access was no longer required. In addition, password controls were not adequately administered to ensure the authentication of all users who had access to civilian pay data. Likewise, password reset capability was not uniformly administered by or adequately restricted to security personnel. Consequently, the integrity of the civilian pay data was at risk (Finding B).
- Inadequate controls existed over Government and contract personnel who had sensitive access to application software and civilian pay data. When this problem was brought to management's attention, corrective actions were taken; however, additional improvements are needed (Finding C).

No instances of fraud or abuse were detected. Because of their sensitive nature, the deficiencies discussed in this report are presented in general terms. Details of the findings and other matters were provided separately to management. For details of the audit results, see the Findings section of the report. See Appendix A for details of the management control program.

Summary of Recommendations. We recommend that the Defense Information Systems Agency perform a security review on the mainframe computers that support the civilian pay application and implement standard system controls in accordance with agency guidance. We further recommend that all positions requiring sensitive access be designated critical-sensitive, and that background investigations be completed on all personnel in these positions. We also recommend that DFAS require users who have access to the pay application to change their password every 90 days. Further, we recommend that DFAS review all inactive users and delete users who no longer need access. We recommend that DFAS modify user authentication programs, establish procedures for issuing and resetting user passwords, and restrict password reset capability to defined security personnel.

Management Comments. The Defense Information Systems Agency concurred with all recommendations. A security review will be performed on the mainframe computer that supports the civilian pay application. This comprehensive review will ensure that all standard settings and security safeguards conform to established guidance. In addition, 90-day minimum password change requirements will be enforced for all users. The Defense Information Systems Agency also stated that sensitive positions assigned to Government and contract personnel at the Defense Information Systems Agency Area Command, Mechanicsburg, will be designated critical-sensitive and background investigations will be obtained for individuals assigned to those positions.

DFAS concurred in principle with three recommendations. The 90-day password change requirement will be established for the majority of civilian pay users. However, nonexpiring passwords will be permitted for agencies that interact with the application only through batch interfaces. Management agreed to delete inactive users after a specified amount of time. Because the second layer of security is unique to civilian pay and is not required, DFAS will remove this layer and rely on the primary security layer controlled by the security software for user authentication and verification. DFAS fully concurred with two recommendations. Management will publish procedures for issuing and resetting passwords for all civilian pay users. Password reset capability will be restricted to the personnel required to perform this function.

Audit Response. The Defense Information Systems Agency comments were partially responsive. Management agreed to designate sensitive positions as critical-sensitive and to obtain background investigations for all personnel assigned to these positions at one location. However, the Defense Information Systems Agency did not respond to similar recommendations concerning personnel assigned to sensitive positions at its Systems Support Office, Dayton. We request that the Defense Information Systems Agency provide comments on those recommendations by June 7, 1999. The DFAS comments were fully responsive, and additional comments are not required. A discussion of management comments is in the Findings section of the report, and the complete text is in the Management Comments section.

Table of Contents

Executive Summary	i
Introduction	
Background	1
Objectives	2
Findings	
A. Adequacy of System Controls	3
B. DCPS Security Controls	8
C. Critical-Sensitive Ratings	13
Appendixes	
A. Audit Process	
Scope	17
Methodology	18
Management Control Program	18
B. Summary of Prior Coverage	20
C. Report Distribution	21
Management Comments	
Defense Finance and Accounting Service Comments	23
Defense Information Systems Agency Comments	27

Background

System Overview. The Defense Civilian Pay System (DCPS) was approved by the Under Secretary of Defense (Comptroller) as the DoD migratory civilian pay system in September 1991. The primary objective of DCPS is to standardize DoD civilian pay and to fulfill all pay-related reporting requirements. To accomplish this, DCPS maintains employee records that contain pay and leave entitlements, deductions, withholdings, time and attendance data, and all other information pertinent to an employee's employment status. DCPS users consist of the Military Departments, the Defense Finance and Accounting Service (DFAS), and other organizations in the Federal Government. DCPS currently services 733,000 payroll accounts and processes payroll transactions valued at more than \$38 billion annually. DCPS was fully implemented in June 1998.

Supporting Organizations. Four DFAS organizations and the Defense Information Systems Agency (DISA) provide support for the DCPS application and mainframe computers.

DFAS Systems Engineering Organization. Software development, design, testing, and other central design support for the DCPS application is provided by the DFAS Systems Engineering Organization (SEO),¹ Pensacola, Florida.

DFAS Payroll Offices. The payroll office at the DFAS Denver Center, Denver, Colorado, and DFAS Operating Locations in Charleston, South Carolina, and Pensacola maintain employee pay records and DCPS account data.

DISA. The DCPS application resides on separate mainframe computers at the DISA Defense Megacenters (DMC) in Mechanicsburg, Pennsylvania, and in Denver.²

- The DCPS processing environment (the WCC³) at DMC Mechanicsburg supports the employee account data maintained by the DFAS Operating Locations in Charleston and Pensacola. DMC Mechanicsburg provides executive software support for this environment.

¹Formerly known as the DFAS Financial Systems Organization, Financial Systems Activity (FSA), Pensacola. This organization was referred to as the DFAS FSA Pensacola in the draft audit report. Because the central design support responsibilities for the DCPS application did not change, the new name of the organization is given in this final report.

²In November 1998, the DCPS account data residing on the DMC Denver mainframe computer migrated to a mainframe located at DMC Mechanicsburg. The issues and related recommendations addressed in this report did not change.

³WCC is used in this report as an identifier for the DCPS production platform at DMC Mechanicsburg.

-
- The DCPS employee account data maintained by the DFAS Denver Center reside on a mainframe computer at DMC Denver. However, the DISA Systems Support Office (SSO), Dayton, Ohio, provides software support for the processing environment, which is known as the CP1. The Dayton SSO reports to the Commander, DMC Mechanicsburg (now the Site Commander, DISA Area Command [DAC], Mechanicsburg).

Security Software. Computer Associates International, Inc., Access Control Facility 2 (CA-ACF2) is the external security software used to protect the CP1 and WCC processing environments. CA-ACF2 provides system security and control over DCPS software, data, and data communications. It identifies the users who have access to the computer systems and defines the resources that the users are authorized to access. When properly implemented, CA-ACF2 ensures that the operating system and application software are protected according to DoD security requirements.

Chief Financial Officers Act of 1990. This audit supports the financial statement audit requirements of Public Law 101-576, the "Chief Financial Officers Act of 1990," November 15, 1990, as amended by Public Law 103-356, the "Federal Financial Management Act of 1994," October 13, 1994. The civilian pay data were reported in the "Department of Defense Agency-wide Financial Statements for FY 1997 Financial Activity, Statement of Operations and Changes in Net Position." Footnote 23 to line item 9, Program or Operating Expenses, lists the actual pay data as "Personal Services and Benefits." DCPS summarizes the total amount paid by each paying office and reports the figures to the appropriate payroll office on the 592 Disbursement Report. The pay data are entered into more than 40 different accounting systems that report the totals through accounting offices to the financial statements.

Objectives

The primary objective of our audit was to determine whether the security software controls adequately safeguarded the integrity of DCPS pay data. We also reviewed the adequacy of the management control program as it applied to the audit objectives. Appendix A discusses the audit scope and methodology and the review of the management control program. Appendix B lists prior audits related to the audit objectives.

A. Adequacy of System Controls

DISA did not maintain adequate system controls over the processing environments that support the DCPS application.

- Global System Option (GSO) settings were not established in accordance with DISA guidance.
- User access to sensitive privileges was not adequately controlled on either CP1 or WCC.
- Password change requirements were not enforced for all users on either CP1 or WCC.

These control weaknesses existed because DISA did not perform security reviews on the mainframe computers that support DCPS. Security controls over the processing environments must be enforced to ensure the integrity of the civilian pay data and the protection of Federal information assets. Inadequate system controls over the GSO settings and user access are a material management control weakness.

Oversight of System Security

Security Readiness Reviews. The DISA Information Security Task Force was established in April 1994 to identify and correct problems with technical implementation of software security measures at the DISA data centers (now the Defense Megacenters). The task force conducts security readiness reviews that emphasize the importance of implementing standard software security measures. The reviews also determine whether data centers are complying with DISA guidance for achieving standard security environments. Security readiness reviews previously scheduled for the CP1 and WCC mainframe computers were delayed until the supporting operating systems could be upgraded. These upgrades were scheduled for FY 1998.

DISA Guidance. Effective system and security controls are required to ensure that all information is properly protected and is available only to users who need it. This requirement, together with the need for uniform implementation of software throughout DISA, led to the development of standard software guidance. The DISA "MVS Security Technical Implementation Guide" (the TIG), December 1997, gives the minimum system and user requirements for ensuring the uniform application of system controls for all DISA MVS⁴ mainframe computers.

⁴MVS is the International Business Machines Multiple Virtual Storage operating system. The MVS operating system provides integrity of the operating environment as part of the trusted computer base.

Global System Option Settings

The TIG prescribes standard values for GSO settings for all DISA operating environments protected by CA-ACF2 security software. These settings contain options that are critical to an effective security environment and allow customization using options for global software configuration. We reviewed selected GSO settings on both CP1 and WCC and found instances of noncompliance.

Sensitive Utilities. The TIG identifies 15 sensitive utilities (protected programs) that require special protection. These programs are required in a data center to support computer operations. The TIG states that these programs are to be protected by listing each program on the GSO record. However, on WCC, 6 of the 15 sensitive utilities were not identified on the GSO as protected. All 15 sensitive programs were listed as protected programs on the GSO record on CP1.

Uncontrolled use of these sensitive utilities presents a potential security exposure that could result in a major system failure or loss of data. Therefore, access to these programs must be restricted to personnel who require access. Access is restricted through a special designation in the CA-ACF2 user ID record. However, on CP1 or WCC, user access to protected programs was not adequately restricted. Specifically, 69 CP1 users and 9 WCC users were granted the protected program privilege. When this problem was brought to the attention of management, DMC Mechanicsburg reviewed and immediately removed sensitive access from seven of the nine WCC users. The Dayton SSO did not comment on the reasonableness of access granted to the 69 users on CP1.

User ID String. A unique user ID identifies each user⁵ to CA-ACF2. To provide CA-ACF2 with greater flexibility in identifying individual users, a user ID string is created and can be uniquely formatted to include information from user-defined fields (such as company code, office, or division). The user ID string is made up of selected field information from the user ID record and allows the grouping of users by any field or combination of fields. The string can be utilized to enhance security controls over groups of users. The TIG defines the DISA standard user ID string and requires each site to ensure that all fields in the string reflect the standard. The user ID string defined for CP1 was in accordance with the DISA standard. However, the string for WCC consisted of four generic fields in addition to the user ID, rather than the defined fields required by the TIG. Management at DMC Mechanicsburg was aware of this discrepancy on WCC, but had not redefined the user ID string.

⁵A user is defined as either an individual accessing a computer resource or a task being executed on the system that requires access to a resource.

User Access Controls

Controlling user access is vital to ensuring that the operating environment and its applications are protected from unauthorized modification or disclosure. These capabilities were not adequately controlled on either CP1 or WCC.

Sensitive Privileges. The TIG identifies sensitive system privileges that must be used only by specific authorized users. These sensitive privileges grant users special capabilities when accessing the CA-ACF2 databases. The specific designation for each sensitive privilege is stored on the individual user ID record. When assigned to the user record, these privileges allow the user to perform a specific sensitive task. These tasks include, but are not limited to, the ability to execute any program; to activate changes to the system that controls GSO records; and to insert, change, list, and delete access records.

We examined nine sensitive privileges assigned to users identified on CP1 and WCC. Of the nine, eight privileges were not adequately controlled on either of the DCPS mainframe computers. For example, the sensitive privilege that allowed a user access to any dataset, regardless of whether or not the user was authorized through access rules, was assigned to 103 users on WCC. This same privilege was restricted to 18 users on CP1. Also, on the CP1, 27 users were granted the sensitive privilege that allowed them to bypass security-related controls to access data on tape. On WCC, this sensitive privilege was restricted to one user.

In addition, CA-ACF2 implementation standards suggest that some combinations of sensitive privileges should not be assigned to any one user. For example, a privilege that allows the user to create and delete user ID records should not be assigned to a user who has the capability to write access and resource rules. This would violate a basic tenet of internal controls: that no one person has complete control. However, 200 DCPS users on WCC were granted the capabilities of both sensitive privileges. These privileges were limited to eight users on CP1.

The TIG requires that when assigning the sensitive privilege that allows a user to perform security functions, the user must also be assigned the privilege that requires validation of the access rule. This criterion was not met for 10 of 13 users on CP1 and 7 of 224 users on WCC. To ensure the integrity of the DCPS operating environments, sensitive privilege capabilities must be reviewed and limited to authorized users. However, DISA had not performed a comprehensive review of access privileges as part of a security readiness review on either CP1 or WCC.

Password Change Requirements. To protect system data and application resources, the TIG states that all users with access to DISA systems are required, at a minimum, to change their CA-ACF2 controlled passwords every 90 days. However, over 180 users on WCC and over 4,100 users on CP1 did not have expiration days established for their passwords. As a result, once the passwords were established, these users were not required to change them. DISA was not aware of this potential exposure because security reviews were not performed on either of the DCPS mainframe computers. DFAS SEO

security personnel can change the password expiration field in the DCPS user ID records. For DMC Mechanicsburg to maintain the password requirement for all users, the DFAS SEO must ensure that the password expiration field is specified at 90 days for all DCPS users. The potential for data manipulation and possible fraud, waste, and abuse is increased if passwords are not periodically changed.

Summary

The TIG provides technical instruction for securing DISA operating environments protected by CA-ACF2 security software. To ensure the integrity of operating system and application resources and data, DISA must strengthen security controls by implementing the standard requirements in the TIG and by limiting user access to system capabilities required to support the users' responsibilities.

Since the conclusion of the audit fieldwork, the CP1 production environment has been moved from Denver to Mechanicsburg. As a result of this move, the WCC and CP1 processing environments were merged. The DISA responses to the audit recommendations pertain to the merged processing environment. Further, during the fieldwork phase of the audit, the DFAS SEO was known as the DFAS Financial Systems Activity, Pensacola, and was addressed as such in the draft report. The central design activity responsibilities for the DCPS application and the issues and related recommendations in this report did not change as a result of the DFAS reorganization. Therefore, recommendations in this report have not been redirected. The new organization title is given in Recommendations A.2. and B.1. through 4.

Recommendations, Management Comments, and Audit Response

A.1. We recommend that the Director, Defense Information Systems Agency:

a. Perform a security review on the mainframe computers that support the Defense Civilian Pay System.

b. Verify that Global System Option settings over the mainframe computers that support the Defense Civilian Pay System are implemented in accordance with the Defense Information Systems Agency "MVS Security Technical Implementation Guide," December 1997. At a minimum:

(1) List all sensitive utilities in the Global System Option record settings.

(2) Review and restrict access to all sensitive utilities to users who require such access.

(2) Review and restrict access to all sensitive utilities to users who require such access.

(3) Redefine the user identification string for WCC as required by the "MVS Security Technical Implementation Guide."

(4) Review and restrict access capability to all sensitive privileges in accordance with the "MVS Security Technical Implementation Guide."

c. Establish 90-day minimum password change requirements for all users on CP1 and WCC, as directed by the "MVS Security Technical Implementation Guide."

Management Comments. DISA concurred, stating that a comprehensive security readiness review would be performed on the DCPS mainframe to determine whether global settings conform to DISA guidance. A plan for corrective action will be developed and completion dates will be established for each discrepancy noted.

A.2. We recommend that the Director, Defense Finance and Accounting Service Systems Engineering Organization, Pensacola, Florida, establish 90-day minimum password change requirements for all civilian pay users on CP1 and WCC.

Management Comments. DFAS concurred in principle, stating that action has been taken to delete inactive passwords. DFAS will take the necessary action to establish the 90-day password change requirement for most users. However, for users who require interaction through batch interfaces, rather than on-line access, nonexpiring passwords will be permitted. Requests for the nonexpiring passwords are strictly reviewed and justified by the DCPS Security Officer and DISA.

Audit Response. The DFAS comments were responsive. We recognize the need for nonexpiring passwords for some unique users. The intent of the recommendation was to address password expiration requirements for interactive, on-line users of DCPS. To ensure the protection of DCPS data, the DFAS SEO must ensure that the 90-day password expiration field is specified for all DCPS users with interactive, on-line access. The action proposed by DFAS satisfies the intent of the recommendation.

DISA Comments. DISA was not required to comment, but expressed its support of the recommendation and agreed to work with DFAS to establish an automated means of ensuring that the 90-day password change requirement is enforced.

B. DCPS Security Controls

Security controls over the DCPS application needed improvement.

- Inactive user IDs were not canceled and subsequently deleted from CP1 or WCC when access to the DCPS application was no longer required.
- Password controls were not adequately administered by the DFAS SEO to ensure the authentication of all users with access to DCPS data.
- Procedures for resetting passwords were not consistent throughout DCPS. In addition, the ability to reset passwords was not adequately restricted to identified security personnel.

The Information System Security Officer (ISSO) for DCPS did not perform regular reviews to ensure that the application was maintained and disposed of in accordance with internal security policies and practices as required by DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988. These inadequate security controls over inactive users, user authentication, and password-reset capabilities constitute a material management control weakness. We did not find instances of unauthorized access or unauthorized software modifications. However, security controls over the DCPS resources and data must be strengthened to ensure the integrity of civilian pay data and the protection of Federal information assets.

DCPS User Controls

Background. DoD Directive 5200.28 gives minimum AIS security requirements for DoD. These requirements include naming an ISSO for each AIS and assigning to the ISSO security responsibility for the AIS. Security control over DCPS was the responsibility of the ISSO at the DFAS SEO. However, the overall DCPS security structure allowed decentralized control of user IDs and passwords for payroll office personnel. DFAS manual DCPS-SG-01, "Defense Civilian Pay System Security Guidelines Manual," August 3, 1997, defines the DCPS security structure and assigns all aspects of payroll office security to the Automated Data Processing Special Security Officer (ADPSSO) designated by the DFAS payroll offices in Charleston, Denver, and Pensacola.

Inactive User IDs. Access to DCPS requires a unique user ID and password for each user. Because inactive user access permissions are more susceptible to compromise, the permissions must be regularly reviewed and removed from the system when user access is no longer required. DCPS-SG-01 gives the ADPSSO at each payroll office the responsibility for adding, canceling, or

deleting user IDs.⁶ However, the ADPSSOs did not cancel, review, and subsequently delete user ID permissions from CP1 or WCC when users no longer had valid needs for access. In addition, the DCPS ISSO did not perform regular reviews to verify that users with access to DCPS had a valid need to know or that the security policies directed by DFAS manual DCPS-SG-01 were followed. As a result, application access was permitted for more than 3,300 inactive user IDs on CP1 and 800 inactive user IDs on WCC. These users had not accessed the application in over 90 days, and many had not accessed the system in more than 1 year. None of the 4,100 inactive user IDs had been canceled. An additional 3,821 user IDs were deleted from WCC during the audit.

The ADPSSO was responsible for all aspects of payroll office security, including maintenance and control of user IDs for each payroll office and its customers. However, this decentralized security structure does not relieve the DCPS ISSO of the responsibility, as mandated by DoD Directive 5200.28, for ensuring that the AIS is maintained and disposed of in accordance with internal security policies and practices. The audit did not review or disclose any instances of unauthorized use of inactive user access permissions. However, the conditions exist, increasing the risk of fraud, waste, and abuse.

User Password Controls. Password controls were not adequately administered by the DFAS SEO to verify user identity for all users with access to DCPS data. Specifically, password controls designed for additional user authentication by DCPS programs did not provide the intended level of security. In addition, password reset capabilities were not adequately restricted, and procedures were not written to ensure uniform implementation DCPS-wide.

User Authentication. Before gaining access to DCPS, every user is required to pass through two levels of password security. The first level is needed to sign on to the DISA mainframe computer. A unique user ID and password, controlled by the CA-ACF2 security software, are required for each user. The second level of password security controls access to DCPS. A set of questions and answers, required by the DCPS application security programs, provides the second level of user authentication. These questions require answers that may be fixed or variable. For example, the question, "What is your mother's maiden name?" requires a fixed response. However, the answer to the question, "What is your favorite food?" may change. Each DCPS user is required to answer all 10 security questions on-line during the initial sign-on. Subsequently, the user must correctly answer 2 of the 10 questions, randomly selected by the security program, to gain access to DCPS. These user authentication controls are intended to provide additional protection for DCPS data, but are ineffective because the users can circumvent them.

- Although logical answers to each of the 10 questions dictate either an alphabetical or numerical response, the security programs do not require logical multicharacter

⁶When a user ID is canceled, the user is denied access to the system until access is reinstated by a security administrator. In contrast, when a user ID is inactive but not canceled, the user ID can be reactivated by resetting the password parameter of the user ID record.

responses. That is, in answer to the question, "What is your favorite food?" a user could respond with the numeric character of 1.

- Likewise, the first-level password required for CA-ACF2 could be used to answer each of the 10 second-level questions.
- The same, single alphabetical or numerical character response can be given to all 10 questions.

DFAS was aware of this control weakness, but did not correct it. Rather, DFAS assumed that each user could be relied on to provide logical responses to the questions. The 10 questions may be too onerous a control, which may encourage users to circumvent it. A more effective password control would be to reduce the 10 questions to a more reasonable number of questions that require a fixed response. In addition, DCPS should be modified to require logical responses to all questions. For example, a question requiring a numerical response should be programmed to reject all alphabetical characters.

Password Reset Procedures. To ensure the integrity of the DCPS data and individual user identity, passwords associated with unique user IDs must be adequately protected and controlled. When signing on, a user is required to replace a predefined password with a unique password of his or her own selection. Security personnel must reset the password if, for example, the user forgets the password or the password is suspended as a result of key entry errors. DFAS manual DCPS-SG-01 assigns password reset responsibilities for DCPS users to the ADPSSO in the DFAS payroll offices at Charleston, Denver, and Pensacola. In practice, however, password reset capability was not limited to the ADPSSO at each payroll office. Over 140 users on CP1 and over 200 users on WCC could reset user passwords. Considering the extensive number of DCPS users worldwide, password reset capability may need to be further delegated. However, when granting this capability to additional users, the capability should be restricted to password resets. Password reset capabilities are controlled and defined by CA-ACF2 sensitive privilege parameters. The sensitive privileges, as currently defined, permit password reset capability in addition to other sensitive tasks, such as the ability to create, change, and delete user IDs. Users with this capability should be limited to password resets.

In addition, detailed password reset procedures were not included in DFAS manual DCPS-SG-01 to ensure that users were adequately identified before allowing passwords to be reset. For example, DFAS manual DCPS-SG-01 did not provide guidelines to adequately verify the identity of a user making a telephone call to request a password reset. As a result, password reset procedures were not uniformly implemented and did not provide the level of user control necessary to ensure that DCPS data and resources were accessed only by authorized users. Because DCPS users are located not only at the DFAS SEO, but also at payroll offices and activities throughout the world, authentication controls are vital to ensure the integrity of DCPS data. These procedures should also be closely monitored by the DCPS ISSO to ensure that the AIS is maintained in accordance with internal security policies and practices, as required by DoD Directive 5200.28.

Management Comments on the Finding

Management Comments. DFAS concurred with all findings except Finding B. Specifically, DFAS stated that password controls were adequately administered by the DFAS SEO to ensure authentication of all users with access to DCPS data. DCPS employs an extra layer of security that forces its users not only to enter a user ID and password, but also to answer 2 of 10 randomly selected questions. The finding is based on the auditor's observations regarding this second layer of security. The first layer ensures the authentication of users in the same manner as other, similar systems. Therefore, the DFAS SEO does not believe the extra layer of security, regardless of the observation made against it, prevented the proper and adequate authentication of all users with access to DCPS data.

Audit Response. The finding stated that password controls designed by the DFAS SEO to provide an extra layer of user authentication did not afford the intended level of security. Rather, these DFAS SEO controls could be, and were, routinely circumvented not only by DCPS users but also by DFAS SEO personnel. The intended controls were tested, not merely observed, by DCPS users within the Inspector General, DoD. As stated in the finding, the controls were determined to be inadequate. The intent of the finding was to alert the DFAS SEO of the weakness and recommend appropriate corrective action. Therefore, the finding and recommendations remain as stated. We agree that the first layer of security provided by CA-ACF2, when properly administered, provides adequate user authentication. However, DFAS SEO placed additional reliance on a second layer of security that did not provide its intended level of control.

Recommendations, Management Comments, and Audit Response

B. We recommend that the Director, Defense Finance and Accounting Service Systems Engineering Organization, Pensacola, Florida, require that:

1. The Defense Civilian Pay System Information Systems Security Officer perform, at a minimum, monthly reviews of all user access permissions to the civilian pay application and immediately delete access for users who no longer have a valid need.

Management Comments. DFAS concurred in principle, stating that the use of an automated process for deleting inactive civilian pay users is under consideration.

DISA Comments. In unsolicited comments, DISA stated that the "MVS Security Technical Implementation Guide" requires inactive user IDs to be deleted after 180 days. The DAC Mechanicsburg automatically deletes user IDs from the security database after 180 days of inactivity. The DAC

Mechanicsburg agreed to work with DFAS to implement this automated, monthly process on the civilian pay platform.

2. Modifications be made to user authentication programs for the Defense Civilian Pay System to require unique, logical, multicharacter responses to security questions.

Management Comments. DFAS concurred in principle. DFAS believes that the first layer of security, based on user IDs and passwords, ensures the proper and adequate authentication of users. Because a substantial work load is associated with maintaining the second layer of DCPS security, DFAS will remove this security layer. Corrective action should be accomplished by May 2000.

Audit Response. The DFAS comments were responsive. We agree that the first layer of CA-ACF2 security, when properly administered, will provide adequate authentication of all users to the DCPS application. Therefore, the action proposed by DFAS satisfies the intent of the recommendation. In its current form, the second layer of DCPS security does not provide the intended level of user authentication. Users could circumvent this layer of security; therefore, removing it entirely should not jeopardize the overall security of the application.

3. Procedures for issuing and resetting passwords for all civilian pay users be defined by the Information Systems Security Officer in the Defense Finance and Accounting Service manual DCPS-SG-01, "Defense Civilian Pay System Security Guidelines Manual," August 3, 1997.

DFAS Comments. DFAS concurred with the recommendation. Procedures for issuing and resetting passwords for all DCPS users will be published in the DCPS manual, "Procedures for Maintenance of DFAS DCPS Production USERIDs."

4. Password reset capability be restricted to specific users for the purpose of resetting passwords only.

DFAS Comments. DFAS concurred with this recommendation. DFAS will review the possibility of limiting reset capability to employing activities and limiting the ability to create, change, or delete user IDs.

DISA Comments. Although not required to comment on the recommendation, DISA agreed that password reset capability should be restricted. DISA will work with DFAS to ensure that personnel who reset passwords are limited to that authority.

C. Critical-Sensitive Ratings

Inadequate security controls existed for 15 of 91 Government and contract personnel with sensitive access to DCPS software and data. Security personnel at DMC Mechanicsburg, the Dayton SSO, and the DFAS SEO did not provide sufficient oversight to ensure that the DoD Regulation 5200.2-R, "Personnel Security Program," January 1987, was followed. In addition, security personnel at DMC Mechanicsburg did not ensure that the requirements of DoD Regulation 5200.2-R were included in the contracts issued for AIS support services for FY 1997. As a result, the integrity of DCPS data was not adequately safeguarded. Inadequate controls over personnel with sensitive system access constitutes a material management control weakness.

Security Requirements

DoD Regulation 5200.2-R requires that the following conditions be met.

- Positions should be classified as critical-sensitive if they give individuals access to computer systems that could be used to cause grave damage to the application or data during its operation or maintenance.
- Background investigations should be completed prior to the appointment of personnel who will occupy critical-sensitive positions.
- A waiver must be obtained from the designated official if an individual is appointed to a critical-sensitive position before a background investigation is completed.

Security personnel should verify that these requirements are met before granting access to an automated information system.

DISA Personnel Controls

At DMC Mechanicsburg and the Dayton SSO, 63 Government and contractor personnel had sensitive access to DCPS software and data. Of the 63 personnel, 13 did not meet the requirements of DoD Regulation 5200.2-R.

DMC Mechanicsburg. Security personnel at DMC Mechanicsburg did not ensure that the requirements of DoD Regulation 5200.2-R were met. Specifically, six Government and four contract personnel with sensitive access to DCPS did not have the required background investigation or an interim waiver on file.

The AIS support contracts for FY 1997 did not require a completed background investigation, but required only that contract personnel obtain a secret clearance. A secret clearance, however, does not require the background investigation directed by DoD Regulation 5200.2-R. The requirements of that Regulation were included in the AIS support contracts for FY 1998.

Dayton SSO. Three contract personnel with sensitive access to DCPS did not have the required background investigation or interim waiver on file. In addition, the position description for one Government employee was not appropriately rated critical-sensitive. These conditions existed because of insufficient oversight by security personnel at the Dayton SSO.

Corrective Actions. When these problems were brought to the attention of management, the following actions were immediately taken.

- DMC Mechanicsburg initiated a background investigation and approved an interim waiver for one Government employee and removed sensitive access for another employee. Favorable background investigations were also completed for four Government employees. In addition, an interim waiver was issued for one contract employee.
- Background investigations were initiated on all three contract personnel identified at the Dayton SSO. Background investigations were completed for two personnel; a waiver was issued for the third.

DFAS Systems Engineering Organization

Of 28 Government and contract personnel with sensitive access to DCPS data, 1 Government employee did not have the required background investigation or interim waiver on file. In addition, the position description for this individual was not properly rated critical-sensitive. This discrepancy is significant because of the circumstances surrounding it. The employee was 1 of 13 personnel at DFAS SEO identified in a prior audit report as requiring a background investigation based on the designated sensitivity of the position.⁷ A followup audit⁸ determined that required background investigations had been initiated for all 13 personnel. However, in August 1995, the Defense Intelligence Agency determined that the employee did not meet the minimum criteria for the requested access to sensitive compartmented information. Based on that determination, in December 1995, DFAS required the DFAS SEO to reassign the individual to a non-critical-sensitive position. Nonetheless, while the background investigation was being adjudicated,⁹ the employee maintained

⁷Inspector General, DoD, Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994.

⁸Inspector General, DoD, Report No. 95-270, "Corrective Actions on System and Software Security Deficiencies," June 30, 1995.

⁹All investigations, whether recommended for approval or denial, are adjudicated. Each adjudication is a common-sense determination based upon consideration of all available information.

unlimited, sensitive access to software and data on the two DCPS mainframe computers. The Director, DFAS SEO, was aware of the status of the investigation, but was unaware of the employee's sensitive access to system resources.

Corrective Actions. When this problem was brought to the attention of management, the DFAS SEO suspended access for the employee with sensitive capabilities on CP1. Subsequently, a background investigation was completed for the employee, and the position description was changed to critical-sensitive.

Repeat Finding. The Inspector General, DoD, has addressed DFAS noncompliance with the requirements of DoD Regulation 5200.2-R in several prior audit reports. The latest, Inspector General, DoD, Report No. 97-203, "Application Controls Over the Defense Joint Military Pay System Reserve Component," August 13, 1997, recommended that the Director, DFAS, require each DFAS Center director and the Deputy Director, Information Management Deputate, DFAS, to provide written assurance that the DFAS organizations under their direction are adhering to DoD Regulation 5200.2-R. Because corrective action on the recommendations has not been completed, no additional recommendations will be made to DFAS at this time.

Maintaining DCPS Integrity

Adhering to DoD Regulation 5200.2-R is important to maintaining the integrity of DCPS. Personnel in critical-sensitive positions have a high level of access to DCPS resources and are not easily subject to management oversight and control. When an employee in a critical-sensitive position has a completed background investigation, management has some assurance that the employee is worthy of public trust.

Recommendations, Management Comments, and Audit Response

C.1. We recommend that the Commanding Officer, Defense Information Systems Agency, Defense Megacenters, Mechanicsburg, Pennsylvania:

a. Designate all sensitive positions as critical-sensitive in accordance with DoD Regulation 5200.2-R, "Personnel Security Program," January 1987.

Management Comments. DISA concurred with the recommendation. DAC Mechanicsburg is adding a statement to the position descriptions to indicate those positions that are designated critical-sensitive.

b. Obtain background investigations, and where appropriate, interim waivers pending completion of background investigations, for all personnel with sensitive access to automated information systems, as required by DoD Regulation 5200.2-R.

Management Comments. DISA concurred and obtained background investigations during the audit for all employees except one. A background investigation is being accomplished on the remaining employee.

c. Prepare all contracts to comply with DoD Regulation 5200.2-R by requiring a background investigation for all contract personnel with critical-sensitive access to automated information systems.

Management Comments. DISA concurred. Contracts were revised to include a paragraph stating that individuals who require critical-sensitive access to automated information systems must have a successfully completed background investigation.

C.2. We recommend that the Chief, Defense Information Systems Agency Systems Support Office, Mechanicsburg, Pennsylvania:

a. Designate all sensitive positions as critical-sensitive in accordance with DoD Regulation 5200.2-R, "Personnel Security Program," January 1987.

b. Obtain background investigations, and where appropriate, interim waivers pending completion of background investigations, for all personnel with sensitive access to automated information systems, as required by DoD Regulation 5200.2-R.

Management Comments. DISA did not comment on recommendations C.2.a. and C.2.b. We request that DISA provide comments in response to the final report.

Appendix A. Audit Process

Scope

Work Performed. We examined selected security controls over DCPS production processing on mainframe computers at the DISA DMCs in Mechanicsburg and Denver. DCPS currently services 733,000 employees and processes more than \$38 billion annually in payroll transactions. To test security rules and features and access authorizations, we used the audit features of the CA-ACF2 security software. We discussed the tests and verified the results with personnel at the DFAS SEO, the DMC Mechanicsburg, and the Dayton SSO. The test results are discussed in the Findings section of this report. We also used the CA-CULPRIT report writer to extract authorization data directly from the CP1 and WCC security databases.

To determine the reliability of security controls over CP1 and WCC production processing and DCPS data, we evaluated:

- implementation of the DISA security guidelines in the "MVS Security Technical Implementation Guide,"
- access controls over DCPS users, and
- the implementation of DoD Regulation 5200.2-R by DISA and DFAS.

Limitations to Audit Scope. Because of the size and complexity of DCPS, we limited our review to security controls over DCPS as discussed above. We did not evaluate the DCPS security controls on a separate National Security Agency computer. We did not conduct a review to determine whether DCPS data had been accessed or modified without proper authorization. We detected no instances of fraud, waste, or abuse.

DoD-wide Corporate-Level Government Performance and Results Act Goals. In response to the Government Performance and Results Act, the Department of Defense has established 6 DoD-wide corporate-level performance objectives and 14 goals for meeting these objectives. This report pertains to achievement of the following objectives and goals.

Objective: Fundamentally reengineer the Department and achieve a 21st century infrastructure. **Goal:** Reduce costs while maintaining required military capabilities across all DoD mission areas. (DoD-6)

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objective and goal.

Objective: Ensure that vital DoD information resources are secure and protected. **Goal:** Assess the information assurance posture of DoD operational systems. (ITM-4.4)

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in DoD. This report provides coverage of the Information Management and Technology high-risk area.

Methodology

Use of Computer-Processed Data. We relied on computer-processed data extracted from the security software database provided by CA-ACF2 for CP1 and WCC. All system testing and use of security software audit tools were accomplished in a controlled environment with management approval. We used automated and manual techniques to analyze system data. Based on those tests and assessments, we concluded that the data were sufficiently reliable to be used in meeting the audit objectives.

Audit Type, Dates, and Standards. This financial-related audit was performed from May 1997 through October 1998. The audit was made in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD, and accordingly included such tests of management controls as were considered necessary.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Management Control Program

DoD Directive 5010.38, "Management Control Program," August 26, 1996, requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of Review of Management Control Program. We reviewed the implementation of the DoD management control program by DISA and DFAS. Specifically, we evaluated the adequacy of management controls over computer security at DMC Mechanicsburg and over DCPS at the DFAS SEO. We also reviewed the results of management's self-evaluation of those controls.

Adequacy of Management Controls. We identified material management control weaknesses, as defined by DoD Directive 5010.38, in security controls over the DCPS CP1 and WCC processing environments at DMC Mechanicsburg. Management controls over standard software settings, user access capabilities, password requirements, and personnel in critical-sensitive positions needed improvement. Implementing Recommendations A.1.a., A.1.b.(1) through (4), A.1.c., C.1.a. through c., C.2.a., and C.2.b. should improve security over DCPS civilian pay resources and data. A copy of the report will be provided to the senior DFAS and DISA officials responsible for management controls.

We also identified material management control weaknesses at the DFAS level, as defined by DoD Directive 5010.38. Improvements were needed in controls over password changes, inactive users, user access authorizations, and password authentication. The integrity and security of the DCPS civilian pay data will be improved by implementing Recommendations A.2. and B.1. through B.4.

Adequacy of Management's Self-Evaluation. Security operations at the DMC Mechanicsburg were identified as part of the Automated Data Processing and Physical Security Office assessable unit. DMC Mechanicsburg assigned a medium risk to that assessable unit. The DMC Mechanicsburg self-evaluation included an evaluation of access controls to systems and data, and also relied on the security readiness reviews on numerous megacenter computers to identify control weaknesses. However, these reviews were not performed on the CP1 or WCC mainframe computers. Because DMC Mechanicsburg did not conduct a security readiness review on either of the DCPS computers, a high level of risk should be assigned to that area. Because the reviews were not performed, DMC Mechanicsburg did not identify or report the material management control weaknesses identified in this audit.

DFAS officials identified civilian pay as an assessable unit and identified the risk associated with civilian pay as medium. DFAS officials did not identify the specific material management control weaknesses identified by this audit because their self-evaluation had a broader, less technical perspective. A high level of risk should be assigned to civilian pay based on the large number and disparity of DCPS users throughout the world, DFAS failure to test security procedures, the decentralization of major security access controls, and the sensitivity of the DCPS pay data.

Appendix B. Summary of Prior Coverage

During the past 5 years, the IG, DoD, issued four reports related to DFAS application controls and security. The problem at DFAS SEO discussed in Finding C, concerning the absence of required background investigations and incorrect position sensitivity ratings, was also discussed in IG, DoD, Report Nos. 97-203 and 96-175. That problem is a repeat finding at DFAS. The reports issued on the prior audits are listed below.

Inspector General, DoD

Report No. 99-107, "Computer Security for the Defense Civilian Pay System," March 16, 1999.

Report No. 97-203, "Application Controls Over the Defense Joint Military Pay System Reserve Component," August 15, 1997.

Report No. 96-175, "Computer Security Over the Defense Joint Military Pay System," June 25, 1996.

Report No. 95-270, "Corrective Actions on System and Software Security Deficiencies," June 30, 1995.

Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994.

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
Director, Defense-Wide Information Assurance Program
Assistant Secretary of Defense (Public Affairs)
Director, Defense Logistics Studies Information Exchange

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
Inspector General, National Security Agency
Director, Defense Systems Management College
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations

Office of Management and Budget
General Accounting Office
National Security and International Affairs Division
Technical Information Center

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform

Defense Finance and Accounting Service Comments



DEFENSE FINANCE AND ACCOUNTING SERVICE

1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

DFAS-HQ/S

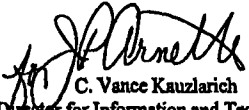
JAN 26 1999

MEMORANDUM FOR DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE,
OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF
DEFENSE

SUBJECT: Audit Report on Computer Security for the Defense Civilian Pay System (Project
No. 7FD-2023.01)

The Defense Finance and Accounting Service (DFAS) comments regarding the draft
audit report, "Computer Security for the Defense Civilian Pay System," dated November 20,
1998, are attached. Comments address those findings and recommendations applicable only to
DFAS, A.2. and B.

My point of contact for this action is Lt Col Jim Pinc, DFAS-HQ/SC, (703) 607-3959.


C. Vance Kauzlarich
Director for Information and Technology

Attachment:
As Stated

cc: DFAS-HQ/F
DFAS-HQ/PO
Director, SEO-PE

**DFAS COMMENTS ON
FINDINGS AND RECOMMENDATIONS
TO DODIG DRAFT REPORT
(PROJECT NO. 7FD-2023.01)**

A. Adequacy of System Controls

Recommendations

A.2. We recommend that the Director, Financial Systems Activity, Financial Systems Organization, Defense Finance and Accounting Service, Pensacola, Florida, establish 90-day minimum password change requirements for all civilian pay users on CP1 and WCC.

DFAS COMMENTS:

Please note that, as a result of a recent reorganization of information and technology services in the Defense Finance and Accounting Service (DFAS), the Financial Systems Organization-Pensacola has been re-designated as the Systems Engineering Organization-Pensacola (SEO-PE). Functions and responsibilities associated with the Defense Civilian Pay System (DCPS) remain the same, so all recommendations as written still apply.

DFAS concurs with Recommendation A.2. in principle. We have taken action to delete current inactive passwords. In addition, DFAS will take the necessary action to establish a 90-day password change requirement for the vast majority of users. However, there are some exceptions (such as the Thrift Savings Board and Federal Reserve Banks) who require a non-expiring password. These agencies do not have on-line access but conduct their interaction through batch interfaces. Since these special case users have no on-line access, they would receive no notification that their password is about to expire at the end of 90 days. To prevent production disruption due to an expired password, these interface partners are issued non-expiring passwords. Requests for these non-expiring passwords undergo a strict review and justification with the Defense Information Services Agency (DISA). A decision on this issue is expected not later than March 15, 1999.

B. DCPS Security Controls

DFAS COMMENTS ON FINDINGS: DFAS concurs with all findings except the second finding, "Password controls were not adequately administered by the DFAS FSA Pensacola to ensure the authentication of all users with access to DCPS data." DCPS augments user authentication with an extra layer of security that few other systems employ. DCPS forces its users to not only enter a userid and password but to also answer two randomly selected questions from a list of ten questions. The finding is based on the auditor's observation regarding this second layer of security. However, the first layer of authentication based on userid and password ensures the authentication of users in the same manner as other similar systems. Therefore, we do not believe that the extra layer of security, regardless of any observations made against it, prevented the SEO-PE from ensuring proper and adequate authentication of all users with access to DCPS data.

Recommendations

B. The Director, Financial Systems Activity, Financial Systems Organization, Defense Finance and Accounting Service, Pensacola, Florida, require that:

1. The Defense Civilian Pay System Information Security Officer perform, at a minimum, monthly reviews of all user access permissions to the civilian pay application and immediately delete access for users who no longer have a valid need.

DFAS COMMENTS: DFAS concurs with Recommendation B.1. in principle. The finding indicated a large number of inactive userids was not deleted from the DCPS database in a timely manner. We are considering various options, including automatically deleting userids that have not been used in DCPS for a specified amount of time. This should eliminate the need for a manual review. A decision on these issues is expected not later than March 31, 1999.

2. Modifications be made to Defense Civilian Pay System user authentication programs to require unique, logical, multicharacter responses to security questions.

DFAS COMMENTS: DFAS concurs with Recommendation B.2. in principle. This recommendation refers to the DCPS practice of using an extra layer of security that is not found in other systems. In addition to entering the userid and password, an individual must also correctly answer two questions randomly selected from a series of ten questions. There is no requirement for this additional layer of security. In addition, we have found that many users have a tendency to forget the answer to the questions. Failure to successfully answer the questions contributes to a significant workload being experienced by the payroll offices to assist the users and reset the password. Since there is no security requirement for this second layer of security and because there is a substantial workload associated with maintaining this level of security, we are removing the requirement for the ten questions. We believe the first layer of security based on userid and password ensures proper and adequate authentication of users. This action should be accomplished by May, 2000.

3. Procedures for issuing and resetting passwords for all civilian pay users be defined by the Information Systems Security Officer in the Defense Finance and Accounting Service DCPS-SG-01, "Defense Civilian Pay System Security Guidelines Manual," August 3, 1997.

DFAS COMMENTS: DFAS concurs with Recommendation B.3. We will publish procedures for issuing and resetting passwords for all civilian pay users in the DCPS manual titled, "Procedure for Maintenance of DFAS DCPS Production USERIDs." Expected completion date is March 19, 1999.

4. Password reset capability be restricted to specific users for the purpose of password resets only.

DFAS COMMENTS: DFAS concurs with Recommendation B.4. We are reviewing the possibility of delegating the password reset capability to the employing activities and limit their ability to create, change and delete userids. A decision on this matter is expected not later than March 31, 1999.

Defense Information Systems Agency Comments



DEFENSE INFORMATION SYSTEMS AGENCY

701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY
REFER TO: Inspector General

22 January 1999

MEMORANDUM FOR DEPARTMENT OF DEFENSE, INSPECTOR GENERAL
ATTN: FINANCE AND ACCOUNTING DIRECTORATE

SUBJECT: Agency Response to DODIG Draft Report, "Computer
Security for the Defense Civilian Pay System"
(Project no. 7FD-2023.01)

Reference: DODIG Draft Audit Report, subject as above,
20 November 1998

1. The Defense Information Systems Agency has reviewed the subject draft report and agrees with the findings and recommendations. Detailed comments are enclosed.
2. My point of contact for this action is Ms. Barbara Nichols, DISA IG/Audit Liaison Team. She can be reached on 703-607-6607.

FOR THE DIRECTOR:

Enclosure a/s


f RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

**DRAFT AUDIT REPORT ON COMPUTER SECURITY
FOR THE DEFENSE CIVILIAN PAY SYSTEM
(PROJECT NO. 7FD-2023.01)**

The DODIG Audit of the Defense Civilian Payroll System (DCPS) was performed on two images, one at Mechanicsburg and the other in Denver. Since the time of the audit fieldwork, the Denver image was migrated to Mechanicsburg, and subsequently the two images were consolidated into a single image. It should be recognized that all audit recommendations will be directed to the single image where all the DCPS processing is now done.

Recommendation A.1: Recommend that the Director, Defense Information Systems Agency:

- a. Perform a security review on the mainframe computers that support the Defense Civilian Pay System.
- b. Verify that Global System Option settings over the mainframe computers that support the Defense Civilian Pay System are implemented in accordance with the Defense Information Systems Agency "MVA Security Technical Implementation Guide," December 1997. At a minimum:
 - (1) List all sensitive utilities in the Global System Option record settings.
 - (2) Review and restrict access to all sensitive utilities to users who require such access.
 - (3) Redefine the user identification string for WCC as required by the "MVS Security Technical Implementation Guide."
 - (4) Review and restrict access capability to all sensitive privileges in accordance with the "MVS Security Technical Implementation Guide."
- c. Establish 90-day minimum password change requirements for all users on CP1 and WCC, as mandated by the "MVS Security Technical Implementation Guide."

Agency Response: Concur. DAC Mechanicsburg supports the recommendation to perform a security readiness review (SRR) of the DCPS image. The review, when performed, will go into much more detail than the audit report, and will result in a plan of action to correct each SRR finding along with a project completion date for each one. The recommendations related to the Global Systems Options will all be addressed during the review and any that are not in compliance with the MVS Security Technical Implementation Guide (STIG) will be addressed. DAC Mechanicsburg is taking a proactive approach to the upcoming SRR review and will attempt to correct as many findings as possible before the formal SRR review is conducted.

Recommendation A2: Recommend that the Director, Financial Systems Activity, Financial Systems Organization, Defense Finance and Accounting Service, Pensacola, Florida, establish 90-day minimum password change requirements for all civilian pay users on CP1 and WCC.

Agency response: DAC Mechanicsburg supports this recommendation, as passwords must be changed every 90 days to comply with the MVS STIG. DAC Mechanicsburg will work with DFAS to establish an automated means for insuring passwords are changed every 90 days.

Recommendation B1: Recommend that the Director, Financial Systems Activity, Financial Systems Organization, Defense Finance and Accounting Service, Pensacola, Florida, require that the Defense Civilian Pay System Information Systems Security Officer perform, at a minimum, monthly reviews of all user access permissions to the civilian pay application and immediately delete access for users who no longer have a valid need.

Agency response: The STIG requires that userids which are inactive after 180 days be deleted, and DAC Mechanicsburg has an automated process in place for other images where a regularly scheduled batch job is run each month to automatically delete userids which have been inactive for 180 days. DAC Mechanicsburg will work with DFAS to implement this process on the DCPS image.

Recommendation B4: Recommend that the Director, Financial Systems Activity, Financial Systems Organization, Defense Finance and Accounting Service, Pensacola, Florida, require that password reset capability be restricted to specific users for the purpose of password resets only.

Agency response: Personnel who are only authorized to reset passwords should be restricted to that authority so that they can not perform any other systems level tasks. DAC Mechanicsburg will work with DFAS to insure those personnel doing resets are limited to only that authority required to do resets.

Recommendation C1 a: We recommend that the Commanding Officer, Defense Megacenter, Defense Information Systems Agency, Mechanicsburg, Pennsylvania designate all sensitive positions as critical-sensitive in accordance with DOD Regulation 5200.2-R, "Personnel Security Program," January 1987.

Agency response: Concur. DAC Mechanicsburg has been including a statement on all SF 52's for positions that are ADP I. We are now in process of adding a statement to the Position Descriptions (PD) to indicate those positions that are ADP I.

Recommendation C1 b. We recommend that the Commanding Officer, Defense Megacenters, Defense Information Systems Agency, Mechanicsburg, Pennsylvania obtain background investigations, and where appropriate, interim waivers pending completion of background investigations, for all personnel with sensitive access to automated information systems, as required by DOD Regulation 5200.2-R.

Agency response: Concur. Action has been completed to obtain SSBI's on all those individuals that were identified in the audit except one. A secret clearance has been granted for the remaining individual and the SSBI investigation is in process.

Recommendation C1 c. We recommend that the Commanding Officer, Defense Megacenters, Defense Information Systems Agency, Mechanicsburg, Pennsylvania prepare all contracts to comply with DOD Regulation 5200.2-R by requiring a background investigation for all contract personnel with critical-sensitive access to automated information systems.

Agency response: Concur. All contracts include a paragraph which states that those individuals who require critical sensitive access have a successfully completed SSBI.

Audit Team Members

The Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD, produced this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.

F. Jay Lane
Brian M. Flynn
W. Andy Cooley
Frances E. Cain
Ben J. Meade
Debra L. Sherwood
Susanne B. Allen